Orbit codes — A new concept in the area of network coding

Trautmann, A L ; Manganiello, F ; Rosenthal, J

Abstract: We introduce a new class of constant dimension codes called orbit codes. The basic properties of these codes are derived. It will be shown that many of the known families of constant dimension codes in the literature are actually orbit codes.

DOI: https://doi.org/10.1109/CIG.2010.5592788

Orbit Codes - A New Concept in the Area of Network Coding

Anna-Lena Trautmann, Felice Manganiello, and Joachim Rosenthal
Institute of Mathematics
University of Zurich
Winterthurerstrasse 190
CH-8057 Zurich, Switzerland
http://www.math.uzh.ch/aa

***Abstract*—We introduce a new class of constant dimension codes called *orbit codes*. The basic properties of these codes are derived. It will be shown that many of the known families of constant dimension codes in the literature are actually orbit codes.**

I. Introduction

In network coding one is looking at the transmission of information through a directed graph with possibly several senders and several receivers. One can increase the throughput by linearly combining the information vectors at intermediate nodes of the network. If the underlying topology of the network is unknown we speak about *random linear network coding*. Since linear spaces are invariant under linear combinations, they are what is needed as codewords [1]. It is helpful (e.g. for decoding) to constrain oneself to subspaces of a fixed dimension, in which case we talk about *constant dimension codes*. Different approaches of constructing constant dimension codes have been investigated, e.g. in [1], [2], [3], [4], [5] and [6].

The structure of the paper is the following: In the second section we give some preliminaries. The main body of the paper is Section 3 where we study actions of discrete groups on the finite Grassmann variety. For this note that one can view a constant dimension code as a discrete subset of the Grassmann variety $\mathcal{G}(k,n)$. We are interested in situations when this discrete subset is also an orbit under the action of a finite group. We call such codes *orbit codes*. Like for linear block codes one has a homogeneity property in the sense that the distance of a code can be determined through the distance of one fixed element with all the other elements.

In Section 4 we show how the Reed-Solomon type codes introduced by Kötter and Kschischang [1] as well as the spread codes described in [7] can be seen as special instances of orbit codes.

II. Preliminaries

Let $\mathbb{F}_q$ be the finite field with q elements (where $q = p^r$ and p prime). The *projective space* $\mathbb{P}^{n-1}$ of dimension $n-1$ over $\mathbb{F}_q$ is the set of all 1-dimensional subspaces of $\mathbb{F}_q^n$, the set of all subspaces of $\mathbb{F}_q^n$ of dimension k is called *Grassmann variety*, denoted by $\mathcal{G}(k,n)$.

It is a well-known result that

$$|\mathcal{G}(k,n)| = \begin{bmatrix} n \\ k \end{bmatrix}_q := \frac{\prod_{i=n-k+1}^{n}(q^i-1)}{\prod_{i=1}^{k}(q^i-1)}$$

Let $U \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ be a full–rank matrix and $\mathcal{U} := \mathrm{rowspace}(U) \in \mathcal{G}(k,n)$. One can notice that for any $T \in \mathrm{GL}_k(\mathbb{F}_q)$

$$\mathcal{U} = \mathrm{rowspace}(U) = \mathrm{rowspace}(TU).$$

The *subspace distance* [1] is a metric on $\mathcal{G}(k,n)$ given by

$$\begin{aligned} d_S(\mathcal{U},\mathcal{V}) &= 2\left(k - \dim(\mathcal{U}\cap\mathcal{V})\right) \\ &= 2\,\mathrm{rank}\begin{bmatrix} U \\ V \end{bmatrix} - 2k \end{aligned}$$

for any $\mathcal{U},\mathcal{V} \in \mathcal{G}(k,n)$ and some respective matrix representations U and V.

A constant dimension code C is simply a subset of the Grassmann variety $\mathcal{G}(k,n)$. The minimum distance is defined in the usual way. A code $C \subset \mathcal{G}(k,n)$ with minimum distance $d_S(C)$ is called a $[n, d_S(C), |C|, k]$-code.

Given $U \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ a full–rank matrix, $\mathcal{U} \in \mathcal{G}(k,n)$ its rowspace and $A \in \mathrm{GL}_n(\mathbb{F}_q)$, we define

$$\mathcal{U}\cdot A := \mathrm{rowspace}(UA).$$

Because of the following lemma, the operation here defined is independent from the representation of $\mathcal{U}$.

Lemma 1: Let $U, U' \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ be matrices such that $\mathrm{rowspace}(U) = \mathrm{rowspace}(U')$. Then $\mathrm{rowspace}(U\cdot A) = \mathrm{rowspace}(U'\cdot A)$ for any $A \in \mathrm{GL}_n(\mathbb{F}_q)$.

We can now define the following group action on the Grassmann variety:

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{F}_q)\times\mathcal{G}(k,n) & \to & \mathcal{G}(k,n) \\ (A,\mathcal{U}) & \mapsto & \mathcal{U}\cdot A \end{array}$$

Proposition 2: The subspace distance is $\mathrm{GL}_n(\mathbb{F}_q)$-invariant.

Proof:

$$d_S(\mathcal{U},\mathcal{V}) = d_S(\mathcal{U}\cdot A, \mathcal{V}\cdot A), \quad \forall A \in \mathrm{GL}_n(\mathbb{F}_q).$$

■

Based on this homogeneity property it will be possible to compute the minimum distance of orbit codes in a simple manner (see Proposition 8).

978-1-4244-8264-1/10/$26.00 © 2010 IEEE

III. Orbit Codes

Definition 3: Let $\mathcal{U} \in \mathcal{G}(k,n)$. Then the stabilizer group of $\mathcal{U}$ is defined as

$$\mathrm{Stab}(\mathcal{U}) := \{A \in \mathrm{GL}_n(\mathbb{F}_q) \mid \mathcal{U}\cdot A = \mathcal{U}\}.$$

This gives rise to an equivalence relation for all $A, B \in \mathrm{GL}_n(\mathbb{F}_q)$ through

$$A \sim B \ :\Longleftrightarrow \ \exists\, S \in \mathrm{Stab}(\mathcal{U}) : A = SB.$$

Theorem 4: For any $\mathcal{U} \in \mathcal{G}(k,n)$ it holds that

$$\mathcal{G}(k,n) \cong \mathrm{GL}_n(\mathbb{F}_q)/\,\mathrm{Stab}(\mathcal{U}).$$

Proof: Fix $U \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ such that $\mathcal{U} = \mathrm{rowspace}(U)$. We prove that the following map is bijective:

$$\begin{array}{rcl} \varphi : \mathrm{GL}_n(\mathbb{F}_q)/\,\mathrm{Stab}(\mathcal{U}) & \to & \mathcal{G}(k,n) \\ [M] & \mapsto & \mathrm{rowspace}(UM), \end{array}$$

where $[M]$ denotes the class in $\mathrm{GL}_n(\mathbb{F}_q)/\,\mathrm{Stab}(\mathcal{U})$ for which $M \in \mathrm{GL}_n(\mathbb{F}_q)$ is a representative.

Consider $\mathcal{V} \in \mathcal{G}(k,n)$ and $V \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ such that $\mathcal{V} = \mathrm{rowspace}(V)$. Then the map is surjective since for any full–rank matrix $V \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ there exists a $M \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $V = UM$.

Let $M_1, M_2 \in \mathrm{GL}_n(\mathbb{F}_q)$. We show that the row space of UM_1 is equal to the row space of UM_2 if and only if $[M_1] = [M_2] \in \mathrm{GL}_n(\mathbb{F}_q)/\,\mathrm{Stab}(\mathcal{U})$:

$$\begin{aligned} &\mathrm{rowspace}(UM_1) = \mathrm{rowspace}(UM_2) \\ &\Longleftrightarrow\ \exists\, M \in \mathrm{GL}_k(\mathbb{F}_q)\ :\ UM_1 = MUM_2 \\ &\Longleftrightarrow\ \mathrm{rowspace}(U) = \mathrm{rowspace}(UM_2M_1^{-1}) \\ &\Longleftrightarrow\ M_2M_1^{-1} \in \mathrm{Stab}(\mathcal{U}) \\ &\Longleftrightarrow\ \exists\, S \in \mathrm{Stab}(\mathcal{U})\ :\ M_2 = SM_1 \\ &\Longleftrightarrow\ [M_1] = [M_2] \end{aligned}$$

This proves that φ is also injective, hence it is a bijection. ∎

Example 5: Consider the case

$$\mathcal{U} = \mathrm{rowspace}\left[\begin{array}{cc} I_{k\times k} & 0_{k\times n-k} \end{array}\right].$$

One verifies that

$$\mathrm{Stab}(\mathcal{U}) = \left\{ \left(\begin{array}{c|c} A_1 & 0 \\ \hline A_2 & A_3 \end{array}\right) \mid A_1 \in \mathrm{GL}_k(\mathbb{F}_q), \right. \\ \left. A_2 \in \mathrm{Mat}_{k\times(n-k)}(\mathbb{F}_q), A_3 \in \mathrm{GL}_{n-k}(\mathbb{F}_q) \right\}.$$

The following proposition shows that any other stabilizer group is conjugated to this special one.

Proposition 6: Let $\mathcal{U}, \mathcal{V} \in \mathcal{G}(k,n)$. Then $\mathrm{Stab}(\mathcal{U})$ is conjugated to $\mathrm{Stab}(\mathcal{V})$. This implies that

$$|\,\mathrm{Stab}(\mathcal{U})| = |\,\mathrm{Stab}(\mathcal{V})|.$$

Proof: Let $A \in \mathrm{GL}_n(\mathbb{F}_q)$ such that $\mathcal{U} = \mathcal{V}\cdot A$. Then $S \in \mathrm{Stab}(\mathcal{U})$ if and only if

$$\mathcal{U}\cdot S = \mathcal{U} \iff (\mathcal{V}\cdot A)\cdot S = \mathcal{V}\cdot A$$

which is equivalent to saying that $ASA^{-1} \in \mathrm{Stab}(\mathcal{V})$. ∎

Definition 7: Let $\mathcal{U} \in \mathcal{G}(k,n)$ be fixed and $\mathfrak{G}$ a subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$. Then

$$C = \{\mathcal{U}\cdot A \mid A \in \mathfrak{G}\}$$

is called an *orbit code*. An orbit code is *cyclic* if the defining group is cyclic.

The name orbit code arises because $\mathfrak{G}$ is a group acting on $\mathcal{G}(k,n)$, i.e. the code is the orbit of the subspace $\mathcal{U}$ under the action of $\mathfrak{G}$.

Proposition 8: Let $C = \{\mathcal{U}\cdot A \mid A \in \mathfrak{G}\}$ be an orbit code. Then it holds that

$$|C| = \frac{|\mathfrak{G}|}{|\mathfrak{G} \cap \mathrm{Stab}(\mathcal{U})|}$$

and

$$d_S(C) = \min_{A \in \mathfrak{G}\setminus \mathrm{Stab}(\mathcal{U})} d_S(\mathcal{U}, \mathcal{U}\cdot A).$$

Moreover $d_S(\mathcal{U}, \mathcal{U}\cdot A_1) = d_S(\mathcal{U}, \mathcal{U}\cdot A_2)$ if $A_1 \sim A_2$.

Proof: The cardinality follows from Proposition 6, whereas the distance between any two elements $\mathcal{V}_1$ and $\mathcal{V}_2$ in the code is

$$d_S(\mathcal{V}_1, \mathcal{V}_2) = d_S(\mathcal{U}\cdot A_1, \mathcal{U}\cdot A_2) = d_S(\mathcal{U}, \mathcal{U}\cdot A_2A_1^{-1})$$

for some $A_1, A_2 \in \mathfrak{G}$. Moreover $A_2A_1^{-1} \in \mathfrak{G}$. ∎

A similar property holds for linear block codes in classical coding theory, where the minimum distance is attained between a non-zero vector and the zero-vector. Hence this can be seen as another analogon of linearity in the subspace setting, different from the one proposed in [8].

Definition 9: If $C \subseteq \mathcal{G}(k,n)$ one defines the *dual code* as

$$C^\perp := \{\mathcal{U}^\perp \in \mathcal{G}(n-k,n) \mid \mathcal{U} \in C\}.$$

We use the name dual to point out the relation with the dual codes in classical coding theory. In [1] this class of codes was first called *complementary codes* and it was shown that if C is a $[n, M, 2\delta, k]$-code then $C^\perp$ is a $[n, M, 2\delta, n-k]$-code.

Theorem 10: The dual code $C^\perp$ of an orbit code C is again an orbit code.

Proof: One immediately verifies that $(\mathcal{U}\cdot A)^\perp = \mathcal{U}^\perp \cdot (A^{-1})^t$. It follows that

$$C^\perp = \{\mathcal{U}^\perp \cdot (A^{-1})^t \mid A \in \mathfrak{G}\}$$

and $\{(A^{-1})^t \mid A \in \mathfrak{G}\} = \{A^t \mid A \in \mathfrak{G}\}$ is again a group. ∎

Proposition 11: Given an orbit code $C = \{\mathcal{U}\cdot A \mid A \in \mathfrak{G}\}$, there exists an isometric orbit code

$$\hat{C} = \{\mathrm{rowspace}\left[\begin{array}{cc} I & 0 \end{array}\right]\cdot A \mid A \in \hat{\mathfrak{G}}\}$$

for some group $\hat{\mathfrak{G}}$. In particular one has

$$|C| = |\hat{C}|$$

and

$$d_S(C) = d_S(\hat{C}).$$

Proof: Let $U \in \mathrm{Mat}_{k\times n}(\mathbb{F}_q)$ be a representation matrix of $\mathcal{U}$, and assume $B \in \mathrm{GL}_n(\mathbb{F}_q)$ to be a matrix such that $UB = \left[\begin{array}{cc} I & 0 \end{array}\right]$. Define the group

$$\hat{\mathfrak{G}} := \{B^{-1}AB \mid A \in \mathfrak{G}\}$$

Then

$$\hat{C} = \{\mathrm{rowspace}\left[\begin{array}{cc} I & 0 \end{array}\right]\cdot A \mid A \in \hat{\mathfrak{G}}\}$$

has the desired properties. ∎

For the rest of the paper let us fix

$$U := \left[\begin{array}{cc} I_{k\times k} & 0_{k\times(n-k)} \end{array}\right]$$

and $\mathcal{U} = \mathrm{rowspace}(U)$.

Proposition 12: Let

$$A = \left(\begin{array}{c|c} A_1 & A_2 \\ \hline A_3 & A_4 \end{array}\right)$$

where $A_1 \in \mathrm{Mat}_{k\times k}(\mathbb{F}_q)$, $A_2 \in \mathrm{Mat}_{k\times(n-k)}(\mathbb{F}_q)$, $A_3 \in \mathrm{Mat}_{(n-k)\times k}(\mathbb{F}_q)$ and $A_4 \in \mathrm{Mat}_{(n-k)\times(n-k)}(\mathbb{F}_q)$. Then

$$UA = \left[\begin{array}{cc} A_1 & A_2 \end{array}\right]$$

and if $A_1 \in \mathrm{GL}_k(\mathbb{F}_q)$

$$d_S(\mathcal{U},\mathcal{U}\cdot A) = k + \mathrm{rank}(A_2)$$

Remark 13: If A_1 is full–rank we can canonically assume $A_1 = I$ because

$$\mathrm{rowspace}\left[\begin{array}{cc} A_1 & A_2 \end{array}\right] = \mathrm{rowspace}\left[\begin{array}{cc} I & (A_1^{-1}A_2) \end{array}\right]$$

IV. Examples

We will now give some examples of orbit codes with good distance properties.

A. Cyclic orbit codes

Over the binary field let $\mathfrak{G}$ be the group generated by

$$G = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{pmatrix}$$

and

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \quad U^{\perp} = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then $\mathrm{Stab}(\mathcal{U})$ is as in Example 5, $\mathrm{order}(G) = 4$ and G, G^2, G^3, G^4 are pairwise not equivalent. One can easily check that $d_S(\mathcal{U},\mathcal{U}\cdot G^i) = 4$ for $i = 1,\ldots,3$, thus $C = \{\mathcal{U}\cdot G^i \mid i = 1,\ldots,4\}$ and $C^{\perp} = \{\mathcal{U}^{\perp}\cdot (G^t)^i \mid i = 1,\ldots,4\}$ are $[4,4,4,2]$-codes.

B. Reed-Solomon-like codes

Gabidulin proved that in the rank distance setting codes of maximal size can be constructed for any given distance [9]. In [1] a Reed-Solomon-like construction for constant dimension codes was introduced and Silva et al. showed that lifting (i.e. concatenating an identity block in front of a matrix and taking the row space) maximum rank distance codes leads to exactly the same codes [4]. The cardinality of Reed-Solomon-like codes is $q^{(n-k)(k-\delta+1)}$ for given ambient space dimension n, subspace dimension k and minimum distance 2δ.

Lemma 14: Let $\mathfrak{H}$ be an additive subgroup of $\mathrm{Mat}_{k\times(n-k)}$ such that all its elements are of rank greater than or equal to $d_S(C)/2$. Furthermore, for any $H_i \in \mathfrak{H}$ let

$$G_i = \left(\begin{array}{c|c} I_{k\times k} & H_i \\ \hline 0 & I_{(n-k)\times(n-k)} \end{array}\right)$$

and $\mathfrak{G}$ be the group generated by all G_i. The resulting orbit code $C = \{\mathcal{U}\cdot A \mid A \in \mathfrak{G}\}$ is a $[n, d_S(C), |\mathfrak{H}|, k]$-code.

Moreover if $\mathfrak{H}$ is a maximum rank distance code, then the orbit code is a Reed-Solomon-like code.

Proof: Any element of $\mathfrak{G}$ has the shape of G. Indeed

$$\left(\begin{array}{c|c} I & H_1 \\ \hline 0 & I \end{array}\right)\cdot\left(\begin{array}{c|c} I & H_2 \\ \hline 0 & I \end{array}\right) = \left(\begin{array}{c|c} I & H_1+H_2 \\ \hline 0 & I \end{array}\right)$$

where, if $H_1, H_2 \in \mathfrak{H}$ then $H_1 + H_2 \in \mathfrak{H}$. Then

$$U\cdot G = \left[\begin{array}{cc} I & H \end{array}\right]$$

and

$$\begin{aligned} d_S(\mathcal{U},\mathcal{U}\cdot G) &= 2\cdot\mathrm{rank}\begin{bmatrix} I & 0 \\ I & H \end{bmatrix} - 2k \\ &= 2\cdot\mathrm{rank}(H) \\ &\geq d_S(C) \end{aligned}$$

The second statement follows from the fact that the resulting code words are of the type $\left[\begin{array}{cc} I & H \end{array}\right]$ (where $H \in \mathfrak{H}$) which corresponds exactly to lifting the maximum rank distance code $\mathfrak{H}$. ∎

C. Spread codes

In the case that $n = j \times k$ Manganiello et al. showed how to construct maximum size codes for maximal minimum distance, i.e. $2\delta = 2k$, as follows [7] : Let P be the companion matrix of a monic primitive polynomial over $\mathbb{F}_q$ of degree k. Then $\mathbb{F}_q[P]$, the $\mathbb{F}_q$-algebra of P, is a field of order q^k and P is a generating element of $\mathbb{F}_q[P]\backslash\{0\}$. The set of all

$$\begin{array}{c} \left[\begin{array}{ccccc} I & P_{i_1} & P_{i_2} & \ldots & P_{i_{j-1}} \end{array}\right] \\ \left[\begin{array}{ccccc} 0 & I & P_{i_1} & \ldots & P_{i_{j-2}} \end{array}\right] \\ \vdots \\ \left[\begin{array}{ccccc} 0 & 0 & \ldots & 0 & I \end{array}\right] \end{array}$$

for $P_m \in \mathbb{F}_q[P]$ is called a spread code. It has minimum distance $2k$ and size $\frac{q^n-1}{q^k-1}$.

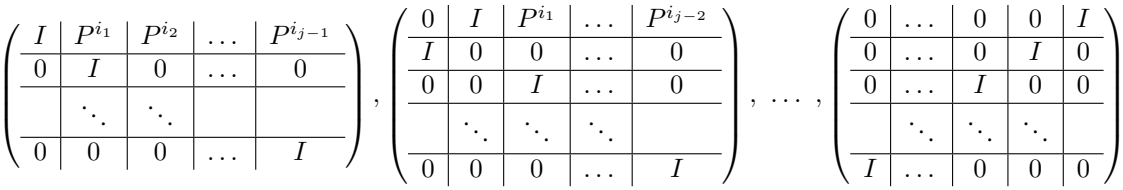

Fig. 1. Generating matrices of the group $\mathfrak{G}$ from Remark 16.

Now let $n = 2k$ and $\mathbb{F}_q[P]$ be the $\mathbb{F}_q$-algebra of P where P is the companion matrix of a monic primitive polynomial over $\mathbb{F}_q$. Moreover, let

$$G_i = \left(\begin{array}{c|c} I & P^i \\ \hline 0 & I \end{array}\right) \qquad G' = \left(\begin{array}{c|c} 0 & I \\ \hline I & 0 \end{array}\right)$$

be the generators of a group $\mathfrak{G}$.

Lemma 15: The resulting orbit code C is the $[n, n, \frac{q^n-1}{q^{n/2}-1}, \frac{n}{2}]$-spread code.

Proof: The blocks are always a linear combination of $0, I$ and elements of $\mathfrak{H}$, thus each block is again an element of $\mathfrak{H}$. Letting $\mathfrak{G}$ act on $\mathcal{U}$, we get spaces represented by $\left[\begin{array}{cc} P^i & P^j \end{array}\right]$.

If P^i is non-zero it holds that

$$\text{rowspace}\left[\begin{array}{cc} P^i & P^j \end{array}\right] = \text{rowspace}\left[\begin{array}{cc} I & (P^i)^{-1}P^j \end{array}\right],$$

hence the elements of C are precisely the row spaces of $\left[\begin{array}{cc} 0 & I \end{array}\right]$ and all $\left[\begin{array}{cc} I & P^i \end{array}\right]$, which is the definition of a spread code. ∎

Remark 16: The construction can be generalized to $n = j \cdot k$ and works for $\mathfrak{H}$ being any subgroup of $\mathrm{GL}_{n/j}(\mathbb{F}_q)$ with field structure. For the construction of a $[n, n, \frac{q^n-1}{q^{n/j}-1}, \frac{n}{j}]$-spread code the generating matrices of $\mathfrak{G}$ are of the shape shown in Fig. 1.

V. Conclusion and Outlook

In this work we introduced *orbit codes* a new class of codes for random network coding. These codes can be described as the discrete orbit under a natural group action within the finite Grassmann variety $\mathcal{G}(k, n)$. We derived the basic properties of these codes. The importance of this class of codes is underlined by the fact that several of the known algebraic construction of constant dimension codes can be seen as orbit codes. E.g. the Reed-Solomon-like codes introduced in [1] as well as the spread codes described [7] can be seen as orbit codes. It is our hope that this approach opens up new possibilities for constructing and decoding constant dimension codes.

In current work we investigate irreducible representations of some of the classical groups and we are interested in the resulting distance properties of the associated orbit codes.

Acknowledgement

The authors were partially supported by Swiss National Science Foundation under Grant no. **126948**.

References

[1] R. Kötter and F. Kschischang, "Coding for errors and erasures in random network coding," *Information Theory, IEEE Transactions on*, vol. 54, no. 8, pp. 3579–3591, August 2008.

[2] T. Etzion and N. Silberstein, "Error-correcting codes in projective spaces via rank-metric codes and Ferrers diagrams," *Information Theory, IEEE Transactions on*, vol. 55, no. 7, pp. 2909–2919, July 2009.

[3] A. Kohnert and S. Kurz, "Construction of large constant dimension codes with a prescribed minimum distance," in *MMICS*, ser. Lecture Notes in Computer Science, J. Calmet, W. Geiselmann, and J. Müller-Quade, Eds., vol. 5393. Springer, 2008, pp. 31–42.

[4] D. Silva, F. Kschischang, and R. Koetter, "A rank-metric approach to error control in random network coding," *Information Theory, IEEE Transactions on*, vol. 54, no. 9, pp. 3951–3967, Sept. 2008.

[5] V. Skachek, "Recursive code construction for random networks," arXiv:0806.3650, 2008.

[6] A.-L. Trautmann and J. Rosenthal, "New improvements on the echelon-ferrers construction," in *Proceedings of the 19th International Symposium on Mathematical Theory of Networks and Systems – MTNS*, Budapest, Hungary, 2010, pp. 405–408.

[7] F. Manganiello, E. Gorla, and J. Rosenthal, "Spread codes and spread decoding in network coding," in *Proceedings of the 2008 IEEE International Symposium on Information Theory*, Toronto, Canada, 2008, pp. 851–855.

[8] T. Etzion and A. Vardy, "Error-correcting codes in projective space," in *Information Theory, 2008. ISIT 2008. IEEE International Symposium on*, July 2008, pp. 871–875.

[9] È. M. Gabidulin, "Theory of codes with maximum rank distance," *Problemy Peredachi Informatsii*, vol. 21, no. 1, pp. 3–16, 1985.